TriCaster 演播室系统与非编网的互联

摘　要：TriCaster 全媒体演播室子系统包含切换系统、视频系统、虚拟演播室系统、音频系统、通话系统、录像系统、同步系统、字幕系统及监视系统。数字化演播室系统具有高集成度、多功能、智能化、灵活性高等特点。本文主要介绍该轻量化演播室的方案、功能特点和安全设计。

关键词：演播室系统

中图分类号：TP37　　**文献标识码：**A

文章编号：1671-0134（2018）05-074-02　　**DOI：**10.19483/j.cnki.11-4653/n.2018.05.020

文 / 王文韬

引言

现代数字化演播室系统，在一台主机上就集成了切换台、调音台、字幕机、多通道硬盘录像机、多轨硬盘录音机、非线性编辑、虚拟演播室、流媒体编码、大屏互动点评、云台摄像机遥控、慢动作播放等演播室主要设备的功能，甚至连演播室周边设备的功能也可以集成进去。但是，集成度的提高，也给系统安全性带来隐患。

1.TriCaster 演播室测试系统的连接

传统的演播室系统，各个设备之间依靠 SDI 等专用通信协议传输数据，在配备冗余设备后，几乎不可能出现单个设备引发整个系统崩溃的情况。而在数字化演播室中，所有设备都通过网络连接在一起，视频播放和字幕系统的素材大多需要通过移动硬盘或 u 盘进入系统，系统的许多功能也要求必须接入互联网才能使用，防止病毒传播和非法进入成为当前安全防范重点。

1.1TriCaster 演播室测试系统的连接方式

测试系统的搭建主要为了评测演播室系统与非编系统的素材交互及日常使用中的安全配置，在保障安全的前提下尽可能多地实现演播室系统的功能，特别是与互联网的交互功能。在系统的连接方式上考虑的三种情况如下。

1.1.1 高度隔离的方式

演播室与非编网两个系统完全独立，系统之间素材的交互通过非编网已有的网闸隔离传输系统进行。这种连接方式的优点是，两个系统完全隔离，不会互相产生影响，现有的系统也不必进行任何更改。缺点是，新建的演播室系统在安全上需要重新设计，素材的导入、导出必须新增隔离传输设备，本地的主备录制系统也需要增加设备，设备投入较大。录制好的素材需要向非编网导入，工作效率低。

1.1.2 两个系统互相融合的方式

这种方式将演播室系统放入非编网内，由非编网的域进行管理，其防病毒和推送补丁由非编网负责。其优点是，素材的导入、导出可以利用非编网的现有设备，节目录制也可以直接写到非编网的素材盘上，既节省投资，也提高了工作效率。但缺点也非常明显，非编和演播室分属不同部门管理，工作协调不易，演播室系统某些功能必须连接互联网，存在安全隐患。

1.1.3 相对独立的连接方式

这种连接方式采用折中的办法，演播室系统与非编网互联时，在级联的交换机端口上进行限制，通过 ACL 配置，只允许指定主机通过指定端口访问非编网的存储节点，拒绝所有其他的连接，再使用组策略限制主机在存储上运行程序和脚本。这样既保证了一定的隔离度，又让演播室系统可以直接将节目写入非编网的素材盘，提高了工作效率。同时，演播室需要的素材也可以通过非编网原有的网闸隔离传输系统导入，节省了设备投入。

1.2 测试系统概述

测试系统使用了 TriCaster 410 作为核心，周边配备了外接的字幕机、录制服务器，以及一台连接互联网，承担互联网应用转发的服务器，这台服务器同时兼顾 windows 补丁分发和网络版杀毒软件的升级和管理。所有的设备通过一台千兆交换机连接在一起。因为测试系统设备较少，没有通过域进行管理，在正式部署时应建立演播室系统的域环境，使管理更加严格、方便、灵活。

在测试系统中，为了提高设备的使用率和工作效率，选择了第三种相对独立的连接方式，演播室系统的交换机和制作网的交换机级联在一起，让演播室系统可以直接读取非编制作的视频，在录制节目时，演播室本地录制一路信号，同时通过网络将另一路信号直接录制到非编的素材盘上，既实现了一主一备的录制，同时又免除了向非编网迁移素材的过程。但是，与编辑网的联通对安全防护提出了更高的要求。

2. 系统的安全设置

在整个系统的安全设置中，主要有以下几个方面：

2.1 病毒防护

为演播室系统的安装网络版杀毒软件。在测试系统中使用了免费的 360 企业版杀毒软件，经测试，软件中的集中管理和升级均可正常使用。软件中还包含了对主机光驱、USB 存储、1394 接口等外挂设备的管理，可以统一禁止各个主机上 usb 存储和光驱的使用，而不影响键鼠等非存储类 USB 设备的使用。

禁止将 U 盘或移动硬盘直接连接到系统内的计算机上。在演播室系统和制作网络连通后，需要上传的素材文件通过制作网现有的网闸上传系统，从办公网或专用上传工作站导入系统内，让素材可以通过一条安全的通道进入系统，避免病毒通过 USB 存储进入系统。通过操作系统的组策略，禁止所有驱动器和非卷设备上的自动播放功能。

在互联网入口配置一体化安全网关 UTM，进行访问控制、病毒防护、防网络攻击。

2. 2 防止非法进入

对登录用户进行限制，防止未授权的访问。所有计算机禁用本机的 administrator 用户，另外建立管理员账户，由演播室技术人员掌握，并定期更改密码。建立权限受限账户，通过组策略设置，隐藏本机盘符并限制用户访问、屏蔽右键的上下文菜单、禁止用户访问控制面板、网络等关键组件。为受限用户定制桌面，只允许运行指定的应用程序。

及时为系统内的计算机推送安全补丁，安全补丁不仅可以堵住非法进入的途径，还可以抑制病毒在网内的传播。由于系统内的设备都使用了 windows 10 操作系统，补丁分发服务要求使用 windows server 2012 以上的服务器版操作系统中集成的 WSUS 服务。操作系统安装完成后，启动服务器管理器，选择添加角色和功能 \windows server 更新服务，系统会同时安装其他一些 WSUS 必须功能，安装成功后还要进行两步配置便可为其他主机推送补丁。（1）编辑组策略，进入计算机配置 \ 策略 \ 管理模板 \ windows 组件 \windows updata\，根据自己的情况配置“配置自动更新”，并在“指定 Intranet Microsoft 更新服务位置”中指定自己的 WSUS 服务器地址；（2）打开 WSUS 管理器，配置好 WSUS 需要更新的产品和分类，指定同步计划和补丁审批，之后便可以开始推送补丁。

2. 3 操作系统加固

账户方面：禁用本地的 administrator 和 Guest 账户，另外新建管理员账户使用。进入组策略：计算机配置 \ windows 设置 \ 安全设置 \ 账户策略，配置密码复杂度、使用期限等策略，配置账户锁定策略。进入安全设置 \ 本地策略 \ 安全选项，启用“网络访问：不允许 SAM 帐户和共享的匿名枚举”，“网络访问：不允许存储网络身份验证的密码和凭证”，禁用“网络访问：允许匿名 SID/ 名称转换”。在“交互式登录中”，启用“不显示最后的用户名”，禁用“无须按 Ctrl+Alt+Del”。如果需要使用来宾账户，配置“账户：重命名来宾账户”为来宾账户改名后使用。

限制受限用户对主机的操作权限：进入组策略用户配置 \ 管理模板 \，尽可能限制“桌面”和““开始”菜单和任务栏”中的项目，只保留用户必须使用的部分。在“网络 \ 网络连接”中，禁止用户对网络属性的访问和更改。在“控制面板”中禁止用户访问控制面板。

在“windows 组件 \windows 资源管理器”中，启用“删除 windows 资源管理器的上下文菜单”可以禁止在系统中使用鼠标右键菜单。启用“隐藏“我的电脑”中这些指定的驱动器”和启用“防止从“我的电脑”访问驱动器”，可以防止用户访问驱动器中的文件，即使使用“运行”对话框也不行。如果想要自己定制需要隐藏的驱动器盘符，需要修改 C：\Windows\PolicyDefinitions 目录下的 WindowsExplorer.admx 和 C：\Windows\PolicyDefinitions\zh-CN 目录下的 WindowsExplorer.adml 两个文件，记住修改前做好备份。

在连接互联网的服务器上，最好关闭系统的默认共享、远程访问注册表、远程桌面等项目，开启防火墙，关闭不必要的服务和端口，启用系统安全审核，并经常进行检查。

2. 4 对人员的安全管理

由于已经使用组策略对受限用户的操作进行限制，这里主要要求技术人员不使用 usb 存储、不连接手机充电、不在系统中安装无关程序。要每天检查系统日志，审核日志等记录，及时发现系统故障和可疑的连接及操作。

结语

不管设置怎么严密，只要有了系统管理员的账号和密码，就对整个系统有了完全控制的权限，所以，一定要保护好自己的系统管理员的账号和密码。媒

参考文献

[1] 孙磊 . Top3DSet 虚拟演播室系统的应用浅析 [J]. 中国传媒科技， 2018（03）：42-43.
[2] 赖慧昌 . 基于 TriCaster 的全媒体小型演播室设计与应用 [J]. 西部广播电视， 2017（15）：195-196.
[3] 孙晋珠 . 新媒体时代的演播室系统设计与建设 [J]. 中国有线电视， 2017（10）：1194-1196.

（作者单位：河南广播电视台）